The G7 Research Group presents the

2021 G7 Cornwall Summit Interim Compliance Report

14 June 2021 to 1 February 2022

Prepared by
Matthew Kieffer and Gabrielle Regimbal
and the G7 Research Group

20 March 2022

www.g7.utoronto.ca
g7@utoronto.ca
@g7_rg

"We have meanwhile set up a process and there are also independent institutions monitoring which objectives of our G7 meetings we actually achieve. When it comes to these goals we have a compliance rate of about 80%, according to the University of Toronto. Germany, with its 87%, comes off pretty well. That means that next year too, under the Japanese G7 presidency, we are going to check where we stand in comparison to what we have discussed with each other now. So a lot of what we have resolved to do here together is something that we are going to have to work very hard at over the next few months. But I think that it has become apparent that we, as the G7, want to assume responsibility far beyond the prosperity in our own countries. That's why today's outreach meetings, that is the meetings with our guests, were also of great importance."

Chancellor Angela Merkel, Schloss Elmau, 8 June 2015

G7 summits are a moment for people to judge whether aspirational intent is met by concrete commitments. The G7 Research Group provides a report card on the implementation of G7 and G20 commitments. It is a good moment for the public to interact with leaders and say, you took a leadership position on these issues — a year later, or three years later, what have you accomplished?

Achim Steiner, Administrator, United Nations Development Programme,
in *G7 Canada: The 2018 Charlevoix Summit*

Contents

19. Digital Economy: Open Internet

"We commit to preserve an open, interoperable, reliable and secure internet, one that is unfragmented, supports freedom, innovation and trust which empowers people."

Carbis Bay G7 Summit Communiqué

Assessment

	No Compliance	Partial Compliance	Full Compliance
Canada			+1
France		0	
Germany			+1
Italy		0	
Japan			+1
United Kingdom			+1
United States			+1
European Union			+1
Average		+0.75 (88%)	

Background

The introduction of the digital sphere into the G7 agenda has been a fairly recent phenomenon. As the digital economy became increasingly relevant to actors' ability to govern, its addition to the agenda became imperative — particularly concerning open and secure internet.[2364] Though the 2021 Cornwall Summit marks the first commitment regarding open internet, the digital economy was first introduced as an issue area in 2000.[2365] The increasing divergence of digital models predicates the existence of a more complex commitment that acknowledges the interaction between economic opportunity, security, ethics, and human rights, as well as the balance between the role of the state, businesses, and individuals. The focus on the digital economy and open internet thus serves to address the regulatory frameworks and relevant stakeholders to ensure a productive and resilient economy in the current data-driven age.[2366]

At the 2000 Okinawa Summit, the Okinawa Charter on Global Information Society marked the first attempt to understand Information and Communication Technologies (ICT) by recognizing the need for universal and affordable internet access for all.[2367] The commitment to bridging the "digital divide" became the primary goal and spurred the creation of the Digital Opportunities Task Force (DOT), which aimed to increase access and connectivity to the internet.[2368]

At the 2011 Deauville Summit, the interactions between proper digital infrastructure and economy were highlighted as G8 leaders aimed to seize emerging opportunities in cloud computing, social networking, and

[2364] OECD Council Recommendation on Principles for Internet Policy Making, Organisation for Economic Co-operation and Development (Paris) 13 December 2011. Access Date: 26 October 2021. https://www.oecd.org/sti/ieconomy/49258588.pdf

[2365] Okinawa Charter on Global Information Society, G8 Information Centre (Toronto) 22 July 2000. Access Date: 26 October 2021

[2366] Carbis Bay G7 Summit Communiqué, G7 Information Centre (Toronto) 13 June 2021. Access Date: 22 September 2021. http://www.g8.utoronto.ca/summit/2000okinawa/gis.htm http://www.g7.utoronto.ca/summit/2021cornwall/210613-communique.html

[2367] Okinawa Charter on Global Information Society, G8 Information Centre (Toronto), 22 July 2000. Access Date: 24 September 2021. http://www.g8.utoronto.ca/summit/2000okinawa/gis.htm

[2368] Digital Opportunities for All: Meeting the Challenge | DOTForce Report Card, G7 Information Centre (Toronto) 1 July 2002. Access Date: 22 September 2021. http://www.g7.utoronto.ca/summit/2002kananaskis/dotforce_reportcard.pdf citizen publications.[2369] The G8 leaders recognized the potential challenges involving interoperability and convergence on public policies concerning personal data, net neutrality, and ICT security.

At the 2013 Lough Erne Summit, G8 leaders introduced an Open Data Charter built on the following main principles: open data by default, transparency about data collection and the release of timely and usable government data while continuing to safeguard privacy.[2370] G8 leaders recognized open government data as an essential resource of the information age that would support the democratic process and increase transparency in financial institutions. The G8 leaders also recognized that free access to open data is of significant value to society and the economy as they have the potential to drive innovation, economic growth, and the creation of jobs.[2371]

At the 2016 Ise-Shima Summit, G7 leaders adopted the G7 Principles and Actions on Cyber, which recognizes digital innovation as essential to the economy and enables transparent policy to stimulate economic growth while promoting privacy and data protection.[2372] Additionally, the leaders aimed to improve connectivity and accessibility by promoting interoperability through ICT standards. The G7 leaders also recognized the Charter of the Digitally Connected World, further emphasizing ICT's role in economic growth and social activities.[2373]

At the 2017 Taormina Summit, G7 leaders recognized the Next Production Revolution (NPR), in which technological and digital advancements revolutionize business and government as a means of increasing economic growth and competitiveness.[2374] Accordingly, the leaders adopted the G7 People-Centered Action Plan on Innovation, Skills and Labor, which promotes access to the digital world while strengthening digital security and promoting Intellectual Property Rights Protections and risk-informed policies that strengthen the digital economy.[2375]

At the 2018 Charlevoix Summit, the G7 leaders committed to the Charlevoix Common Vision for the Future of Artificial Intelligence, which aims to build new forms of economic growth while maintaining an open and fair market environment with certain data protection from artificial intelligence (AI) innovation.[2376] The leaders also recognized the need for internet service providers and social media platforms to improve transparency, which would prevent the illegal use of personal data and breaches of privacy while stimulating the economy.[2377]

At the 2019 Biarritz Summit, G7 leaders agreed on the Biarritz Strategy for an Open, Free and Secure Digital Transformation, which recognizes the internet as a key enabler for economic growth and acknowledges the

[2369] G8 Declaration: Renewed Commitment for Freedom and Democracy, G7 Information Centre (Toronto) 27 May 2011. Access Date: 22 September 2021. http://www.g7.utoronto.ca/summit/2011deauville/2011-declaration-en.html

[2370] 2013 Lough Erne Leaders Communiqué, G7 Information Centre (Toronto) 18 June 2013. Access Date: 24 September 2021. http://www.g7.utoronto.ca/summit/2013lougherne/lough-erne-communique.html

[2371] G8 Open Data Charter, G7 Information Centre (Toronto) 18 June 2013. Access Date: 22 September 2021. http://www.g7.utoronto.ca/summit/2013lougherne/lough-erne-open-data.html

[2372] G7 Principles and Actions on Cyber, G7 Information Centre (Toronto) 27 May 2016. Access Date: 22 September 2021. http://www.g7.utoronto.ca/summit/2016shima/cyber.html

[2373] Charter for the Digitally Connected World, G7 Information Centre (Toronto) 30 April 2016. Access Date: 22 September 2021. http://www.g7.utoronto.ca/ict/2016-ict-charter.html

[2374] G7 Taormina Leaders' Communiqué, G7 Information Centre (Toronto) 27 May 2017. Access Date: 23 September 2021. http://www.g7.utoronto.ca/summit/2017taormina/communique.html

[2375] G7 People-Centered Action Plan on Innovation, Skills and Labor, G7 Information Centre (Toronto) 7 May 2017. Access Date: 23 September 2021. http://www.g7.utoronto.ca/summit/2017taormina/action-plan.html

[2376] Charlevoix Common Vision for the Future of Artificial Intelligence, G7 Information Centre (Toronto) 9 June 2018. Access Date: 23 September 2021. http://www.g7.utoronto.ca/summit/2018charlevoix/ai-commitment.html

[2377] Charlevoix Commitment on Defending Democracy from Foreign Threats, G7 Information Centre (Toronto) 9 June 2018. Access Date: 23 September 2021. http://www.g7.utoronto.ca/summit/2018charlevoix/democracy-commitment.html need to stop malign online behaviour.[2378] The document emphasizes the importance of freedom of expression and opinion, but also addresses the internet's negative effects, including threatening democratic values and stifling economic development. The G7 leaders also formed the G7 and Africa Partnership, which aims to support the reduction of the digital divide and create a more open internet.[2379]

At the 2021 Cornwall Summit, G7 leaders discussed the need for a digital ecosystem that would reflect democratic values and drive innovation across the global economy.[2380] The leaders recognized that cyberspace will determine the future prosperity and wellbeing of people all over the world, and committed to promoting worldwide digital literacy, strengthening digital global norms, and opposing internet shutdowns and network restrictions. The leaders also endorsed the G7 Compact on Research Collaboration and its commitment to protecting research and innovation across the G7 to open research collaboration.

Commitment Features

At the 2021 Cornwall Summit, leaders committed to "preserve an open, interoperable, reliable and secure internet, one that is unfragmented, supports freedom, innovation and trust which empowers people." This commitment can be interpreted as having one main target, which is the preservation of the internet. This target includes six dimensions to preserve: "open," "interoperable," "reliable," "secure," "unfragmented," and "supports freedom, innovation and trust which empowers people."

"Preserve" is understood to mean keeping something safe or protecting it from harm or loss.[2381] In the context of the commitment, it refers to the protection of the aforementioned six dimensions.

In the context of the commitment, "open" is understood to mean unrestricted access to the internet.[2382] This includes free access to the World Wide Web that is available without variables that depend on the financial motives of Internet Service Providers.

"Interoperable" is understood to mean the ability of different digital services to work together and communicate with one another.[2383] In the context of the internet, it refers to users and organizations being able to interact with one another across platforms and efficiently exchange information. An example of compliance can include a government mandating open interfaces.

"Secure" is understood to mean protected from danger or harm.[2384] In the context of the internet, it refers to a connection that is encrypted by one or more security protocols to ensure the security of flowing data.[2385]

[2378] Biarritz Strategy for an Open, Free and Secure Digital Transformation, G7 Information Centre (Toronto) 26 August 2019. Access Date: 24 September 2021. http://www.g7.utoronto.ca/summit/2019biarritz/biarritz-strategy-for-digital-transformation.html

[2379] Biarritz Declaration for a G7 & Africa Partnership, G7 Information Centre (Toronto) 26 August 2019. Access Date: 23 September 2021. http://www.g7.utoronto.ca/summit/2019biarritz/biarritz-declaration-africa-partnership.html

[2380] Carbis Bay G7 Summit Communiqué: Our Shared Agenda for Global Action to Build Back Better, G7 Information Centre (Toronto) 13 June 2021. Access Date: 23 September 2021. http://www.g7.utoronto.ca/summit/2021cornwall/210613-communique.html

[2381] Preserve, Merriam-Webster (Springfield) n.d. Access Date: 26 October 2021. https://www.merriam-webster.com/dictionary/preserve

[2382] Compliance Coding Manual for International Institutional Commitments, G7 and G20 Research Groups (Toronto) 12 November 2020. Access Date: 23 September 2021. http://www.g7.utoronto.ca/compliance/Compliance_Coding_Manual_2020.pdf

[2383] Data portability, interoperability and digital platform competition, Organisation for Economic Co-operation and Development (Paris) n.d. Access Date: 24 September 2021. https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf

[2384] Secure, Merriam-Webster (Springfield) n.d. Access Date: 25 September 2021. https://www.merriam-webster.com/dictionary/secure

[2385] The OECD Privacy Framework, Organisation for Economic Co-operation and Development (Paris) 2013. Access Date: 26 October 2021. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Examples of compliance can include allocating money to information technology training and collaborating with the private sector to share intelligence on and prevent cyber attacks.

"Unfragmented" is often closely linked to "interoperable," and is understood to mean every device on the internet being able to exchange data packets with any other device that is willing to receive them.[2386] Examples of compliance can include preventing fragmentation by monitoring activity on the dark web.

"Support" is understood to mean the action, or act of providing aid, assistance, or backing up an initiative, or entity.[2387] In the context of the commitment, it refers to the internet backing up freedom, innovation, and trust which empowers people.

"Freedom" is understood to mean the absence of necessity, coercion, or constraint in choice or action and the power to choose what one wants to do.[2388] In the context of the commitment, it refers to the right to have unrestricted access to information and the right to privacy, expression, opinion, and innovation.

"Innovation" is understood as the embodiment of an idea in a technology, product, or process that is new and creates value.[2389] An innovation is the implementation of a new or significantly improved product (good or service), or process which derives from creative ideas, technological progress, a new marketing method, a new organizational method in business practices, workplace organization or external relations. Innovation covers a wide range of domains with science and technology as the core.

"Trust" is understood as a person's belief that another person or institution will act consistently with their expectations of positive behaviour.[2390] It is essential for ensuring compliance with regulations, implementing reforms, and enabling people's meaningful participation in civic and political life.

"Empowers" is understood to mean giving powers to someone, including legal power and influence.[2391] Influence can include having the capacity to affect the character or development of someone or something, including oneself.

Full compliance, or a score of +1, will be assigned to G7 members who exemplify demonstrable strong action in at least five of the six dimensions of the target to preserve the internet. This can include both domestic and international actions. Examples of strong actions include, but are not limited to: enforcement of laws through policy action, such as fines for disobeying government guidelines; changing legislation to bring internet-based media services under the democratic oversight of a legitimate government; and money allocation, such as improving infrastructure to connect more citizens to a reliable internet connection. On the international level, strong action can include, but is not limited to: providing financial support to bring broadband access to communities that face barriers to internet access and joining and/or participating in an international organization dedicated to preserving the internet and its dimensions, such as providing affordable internet access worldwide.

[2386] Internet Fragmentation: An Overview, World Economic Forum (Cologny) January 2016. Access Date: 24 September 2021. http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

[2387] Compliance Coding Manual for International Institutional Commitments, G7 and G20 Research Groups (Toronto) 12 November 2020. Access Date: 26 October 2021 http://www.g7.utoronto.ca/compliance/Compliance_Coding_Manual_2020.pdf

[2388] Freedom, Merriam-Webster (Springfield) n.d. Access Date: 26 October 2021. https://www.merriam-webster.com/dictionary/freedom

[2389] Compliance Coding Manual for International Institutional Commitments, G7 and G20 Research Groups (Toronto) 12 November 2020. Access Date: 26 October 2021 http://www.g7.utoronto.ca/compliance/Compliance_Coding_Manual_2020.pdf

[2390] Government at a Glance 2019, Organisation for Economic Co-operation and Development (Paris) n.d. Access Date: 26 October 2021. https://www.oecd-ilibrary.org/docserver/8ccf5c38-en.pdf

[2391] Empower, Merriam-Webster (Springfield) n.d. Access Date: 25 September 2021. https://www.merriam-webster.com/dictionary/empower

Partial compliance, or a score of 0, will be assigned to G7 members who exemplify demonstrable action in only two to four of the six dimensions to preserve the internet, and can include both strong and weak, and domestic and international actions. Examples of weak actions include, but are not limited to, attending meetings that speak on the importance of preserving the internet and any of the six dimensions, verbally reaffirming commitment to the development of the internet or denouncing internet shutdowns, and sharing information about cybercrime and methods of preserving the internet with other G7 members.

Non-compliance, or a score of −1, will be assigned if one of the following scenarios take place: the G7 member exemplifies demonstrable action in one or fewer dimensions to preserve the Internet, or the G7 member fails to take any strong steps towards preserving any of the six dimensions. For example, if a member becomes aware of an increase in domestic cyberattacks but does not implement legislation or programs in efforts to prevent it, then action is not being taken to preserve the "secure" dimension of the Internet.

Scoring Guidelines

−1	The G7 member has NOT taken action to preserve an open, interoperable, reliable, secure and unfragmented internet which empowers people OR has taken action in only one of the aforementioned six dimensions.
0	The G7 member has taken action to preserve two to four of the following six dimensions of the internet: 1) open, 2) interoperable, 3) reliable, 4) secure, 5) unfragmented, and 6) supports freedom, innovation and trust which empowers people.
+1	G7 member has taken strong action to preserve at least five of the following six dimensions of the internet: 1) open, 2) interoperable, 3) reliable, 4) secure, 5) unfragmented, and 6) supports freedom, innovation and trust which empowers people.

Compliance Director: Sofia Shatrova
Lead Analyst: Keah Sharma

Canada: +1

Canada has fully complied with its commitment to preserve an open, interoperable, reliable and secure internet, one that is unfragmented, supports freedom, innovation and trust which empowers people.

On 16 July 2021, the Communications Security Establishment published the 2021 update to its report on Cyber Threats to Canada's Democratic Process.[2392] The update informs Canadians of possible cyber threats against the Canadian electoral process and procedures meant to safeguard its integrity.

On 29 July 2021, Canadian Heritage presented a technical paper on the Government's approach to "address harmful content online."[2393] The paper allows the public to stay up to date with legislative changes that could influence their usage of the internet.

On 16 November 2021, the Canadian Centre for Cyber Security published a Cyber Threat Bulletin.[2394] The publication aims to educate the public on cyberthreats, their development and how to maintain safe internet usage.

[2392] 2021 update on cyber threats to Canada's democratic process, Government of Canada (Ottawa) 16 July 2021. Access Date: 11 October 2021. https://www.canada.ca/en/communications-security/news/2021/07/2021-update-on-cyber-threats-to-canadas-democratic-process.html

[2393] The Government's proposed approach to address harmful content online, Government of Canada (Ottawa) 29 July 2021. Access Date: 11 October 2021. https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html

[2394] Cyber threat bulletin: The ransomware threat in 2021, Canadian Center for Cyber Security (Ottawa) 9 December 2021. Access Date: 10 December 2021. https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-ransomware-threat-2021

On 22 November 2021, Minister of Innovation, Science and Industry François-Philippe Champagne announced a partnership between the Government of Canada and the European Commission to examine the use of digital credentials.[2395] The partnership aims to promote the interoperability of digital credentials and improve the safety of businesses and individuals working online.

On 6 December 2021, Minister of National Defence Anita Anand, Minister of Emergency Preparedness Bill Blair, Minister of Public Safety Marco Mendicino and Minister of International Trade, Export Promotion, Small Business and Economic Development Mary Ng signed an open letter urging Canadian organizations to adopt cyber security practices against ransomware and cybercrime.[2396] The security practices aim to protect business' data and intellectual property.

On 17 December 2021, the Government of Canada launched an open consultation to the public to ensure that all Canadians have access to high-quality wireless services.[2397] The consultation aims to give the public an opportunity to give input for additional provisions to support Canada's Connectivity Strategy and will allow Canadians to get their questions answered by Innovation, Science and Economic Development Canada on the topic of high-quality wireless services. The consultation specifically seeks input on requirements that should be imposed on license holders and measures to support competition among wireless internet providers.[2398]

On 22 December 2021, the President of the Treasury Board Mona Fortier released the interim "What We Heard" report.[2399] The report reviews the first phase of engagement and consultations undertaken as part of the review of access to information and promotes progress tracking and transparent communication to the public.

Canada has fully complied with its commitment to preserve an open, interoperable, reliable and secure internet, one that is unfragmented, supports freedom, innovation and trust which empowers people. Canada has improved cyber threat security and interoperability of internet-based technologies through several partnerships and publications. Additionally, Canada has fostered informed and secure internet use for businesses and public users through open communication.

Thus, Canada receives a score of +1.

Analyst: Anastasiia Bondarenko

[2395] Government of Canada announces partnership with the European Commission to examine the use of digital credentials, Government of Canada (Ottawa) 22 November 2021. Access Date: 28 November 2021. https://www.canada.ca/en/innovation-science-economic-development/news/2021/11/government-of-canada-announces-partnership-with-the-european-commission-to-examine-the-use-of-digital-credentials.html

[2396] Ministers urge Canadian organizations to take action against ransomware, Communications Security Establishment Canada (Ottawa) 6 December 2021. Access Date: 10 December 2021. https://www.canada.ca/en/communications-security/news/2021/12/ministers-urge-canadian-organizations-to-take-action-against-ransomware.html

[2397] Government of Canada launches consultation to ensure Canadians have access to high-quality wireless services, Innovation, Science and Economic Development Canada (Ottawa) 20 December 2021. Access Date: 24 December 2021. https://www.canada.ca/en/innovation-science-economic-development/news/2021/12/government-of-canada-launches-consultation-to-ensure-canadians-have-access-to-high-quality-wireless-services.html

[2398] Government of Canada launches consultation to ensure Canadians have access to high-quality wireless services, Innovation, Science and Economic Development Canada (Ottawa) 20 December 2021. Access Date: 24 December 2021. https://www.canada.ca/en/innovation-science-economic-development/news/2021/12/government-of-canada-launches-consultation-to-ensure-canadians-have-access-to-high-quality-wireless-services.html

[2399] Government of Canada releases first interim report on access to information review, Treasury Board of Canada Secretariat (Ottawa) 22 December 2021. Access Date: 24 December 2021. https://www.canada.ca/en/treasury-board-secretariat/news/2021/12/government-of-canada-releases-first-interim-report-on-access-to-information-act-review.html

France: 0

France has partially complied with its commitment to preserve an open, interoperable, reliable, and secure internet that is unfragmented, supports freedom, innovation and trust which empowers people.

On 13 September 2021, France's Regulatory Authority for Electronic Communications, Posts and Press Distribution (ARCEP) announced a plan to allocate two new mobile network frequency bands in French overseas territories.[2400] The frequency bands are intended to meet increasing demand for access to reliable and efficient mobile services. The plan will increase user connectivity and may lead to fixed internet access offers from mobile networks.

On 30 September 2021, the government of France issued Decree No. 2021-1281.[2401] The decree specifies the obligations of electronic communications operators to report to ARCEP and allows ARCEP to impose interoperability obligations on providers whose interoperability between end-users is compromised.

On 10 November 2021, Minister of Public Sector Transformation and the Civil Service of France Amélie de Montchalin announced a new action plan for open source software in the public sector.[2402] The plan will set up an Open Source Program Office within the public administration and aims to increase the use of digital commons in the administration and support the use of open source codes in France's public sector.

France has partially complied with its commitment to preserve an open, interoperable, reliable, and secure internet, one that is unfragmented, supports freedom, innovation and trust which empowers people. France promoted an open, interoperable, reliable and secure internet by bolstering ARCEP's regulatory power. However, France failed to take significant actions to promote an internet that is unfragmented and which supports innovation and trust which empowers people.

Thus, France receives a score of 0.

Analyst: Selina Zeng

Germany: +1

Germany has fully complied with its commitment to preserve an open, interoperable, reliable and secure internet, one that is unfragmented, supports freedom, innovation and trust which empowers people.

On 30 June 2021, the Cabinet adopted the Third National Action Plan 2021-2023 to improve the digital sovereignty of the administration.[2403] The plan includes the creation of a joint development portal for free software, improving access to information on federal law and increasing transparency of government action.

On 7 July 2021, the German government created a framework for action to improve the government's "open data ecosystem" with the adoption of the "Open Data Strategy."[2404] The Strategy includes 68 measures across

[2400] Frequencies - Overseas, France's Regulatory Authority for Electronic Communications, Posts, and Press Distrubution (Paris) 13 September 2021. Translation provided by Google Translate. Access Date: 29 January 2022. https://www.arcep.fr/actualites/les-communiques-de-presse/detail/n/frequences-outremer-130921.html

[2401] Decree No. 2021-1281 of September 30, 2021 amending the obligations of electronic communications operators in accordance with the European Electronics Communications Code, Government of France (Paris) 30 September 2021. Translation provided by Google Translate. Access Date: 29 January 2022. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044154154

[2402] French Minister announces new plan for supporting open source, European Commission (Brussels) 14 December 2021. Access Date: 29 January 2022. https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/new-action-plan-open-source-french-administration

[2403] Boosting transparency and involvement, The Federal Government (Berlin) 30 June 2021. Access Date: 17 January 2022. https://www.bundesregierung.de/breg-en/service/open-government-partnership-1938274

[2404] Open Data – Driving Success in Innovation, The Federal Government (Berlin) 7 July 2021. Access Date: 17 January 2022. https://www.bundesregierung.de/breg-en/service/open-data-strategy-1940558 three action areas: creating powerful and sustainable data infrastructures, enhancing the innovative and responsible use of data and establishing a "data culture."

On 9 July 2021, the Ministry for Economic Affairs and Energy launched its call for expressions of interest from companies and projects that seek to participate in the Important Project of Common European Interest on Next Generation Cloud Infrastructure and Services (IPCEI-CIS).[2405] Minister for Economic Affairs and Energy Peter Altmaier affirmed that the IPCEI-CIS would help setup an "efficient next generation cloud infrastructure" for Europe. The German government has allocated EUR750 billion to the IPCEI-CIS in support of Europe's "digital sovereignty."

On 8 September 2021, the German government adopted the Cyber Security Strategy for Germany 2021, a long-term plan for the government's cyber security policy.[2406] The strategy includes four overarching guidelines: establishing cyber security as a joint task of the state, business, society and science, strengthening the digital sovereignty of the aforementioned spheres, ensuring the secure development of digitalization and making targets measurable and transparent.

Germany has fully complied with its commitment to preserve an open, interoperable, reliable and secure internet, one that is not fragmented, supports freedom, innovation and trust. Germany has taken steps to preserve an open and secure internet by improving access to reliable information, promoting innovative and open data infrastructures and adopting a comprehensive cyber security strategy.

Thus, Germany receives a score of +1.

Analyst: Arees Chooljian

Italy: 0

Italy has partially complied with its commitment to preserve an open, interoperable, reliable and secure internet that is unfragmented, supports freedom, innovation and trust which empowers people.

On 4 August 2021, the Official Gazette published Decree No. 82.[2407] The Decree contains urgent provisions on cybersecurity, a definition of national cybersecurity and the establishment of the National Cybersecurity Agency by Law No. 109.

On 4 November 2021, the Ministry of Foreign Affairs and International Cooperation and the Presidency of the Council of Ministry of Defense compiled a position paper on "International Law and Cyberspace."[2408] The paper outlines Italy's views concerning the application of international law to cyberspace, including non-intervention and the protection of sovereignty, state accountability in the cyberspace, the application of international human rights law, the role of private stakeholders and international cooperation.

Italy has partially complied with its commitment to preserve an open, interoperable, reliable and secure internet that is unfragmented, supports freedom, innovation and trust which empowers people. Italy has

[2405] Cloud IPCEI entering next phase as call for expressions of interest is launched in Germany and preparations for European matchmaking process get underway, Federal Ministry for Economic Affairs and Climate Action (Berlin) 9 July 2021. Access Date: 13 January 2022. https://www.bmwi.de/Redaktion/EN/Pressemitteilungen/2021/07/20210709-cloud-ipcei-entering-next-phase.html

[2406] Goals adopted in the area of cyber security, The Federal Government (Berlin) 8 September 2021. Access Date: 17 January 2022. https://www.bundesregierung.de/breg-en/service/new-cyber-security-strategy-1958688

[2407] Italy: New cybersecurity law comes into force, OneTrust Dataguidance (Atlanta) 6 August 2021. Access Date: 3 December 2021. https://www.dataguidance.com/news/italy-new-cybersecurity-law-comes-force

[2408] Conference on 'The Application of International Law on Cyberspace' organised at the University of Bologna, EU Cyber Direct (Brussels) 12 November 2021. Access Date: 30 January 2022. https://eucyberdirect.eu/news/conference-on-the-application-of-international-law-to-cyberspace-organized-at-the-university-of-bologna taken action to preserve an open and secure internet by establishing the National Cybersecurity Agency and engaging in international discourse regarding international law and the cyberspace. However, Italy has failed to take action to preserve an interoperable and reliable internet that is unfragmented, supports freedom, innovation and trust which empowers people.

Thus, Italy receives a score of 0.

Analyst: Anastasiia Bondarenko

Japan: +1

Japan has fully complied with its commitment to preserve an open, interoperable, reliable and secure internet, one that is unfragmented, supports freedom, innovation and trust which empowers people.

On 21 June 2021, the Ministry of Economy, Trade and Industry announced the publishing of an international standard that aims to ensure the safety and security of "Internet of Things" (IoT) systems based on IoT Security Guidelines and IoT Safety/Security Development Guidelines.[2409] The standard will contribute to the "safe and secure" development and maintenance of IoT products and services in the digital world.

On 1 September 2021, the Cabinet of Japan formed the Digital Agency.[2410] The Digital Agency aims to digitize public administrative procedures, promote the "standardization and coordination of data systems" and respond to the digital divide.[2411] This response will improve data linkage across separate government organizations and increase their efficiency.

On 11 September 2021, Japan and Vietnam signed an agreement that sees Japan providing Vietnam with defense equipment and technology to promote military and cyber security cooperation between the two countries.[2412] The agreement will control technology transfers between Japan and Vietnam, especially technology transferred to third parties.

On 13 December 2021, Japan, the United States and Australia announced funding for the development of advanced 5G telecommunications networks in the South Pacific region through the construction of a new undersea cable to improve internet connectivity to Micronesia, Nauru and Kiribati.[2413] The initiative aims to avoid situations in which "democracy is threatened by China's control of [Japan's] telecommunications networks."

On 24 December 2021, Prime Minister Fumio Kishida held the second meeting of the Digital Society Promotion Council.[2414] At the meeting, Prime Minister Kishida and other participants discussed the Priority Policy Program for Realizing the Digital Society and set out principles, strategies and measures to realize it with a number of digital reforms through the 2025 fiscal year. Among other goals, the policy program will support both public and private sectors in using digitalization to enhance efficiency and creativity.

[2409] New International Standard for Safe Use of IoT Products and Systems Issued, Ministry of Economy, Trade and Industry (Tokyo) 21 June 2021. Access Date: 14 January 2022. https://www.meti.go.jp/english/press/2021/0621_003.html

[2410] Digital Society Promotion Council, Prime Minister of Japan and His Cabinet (Tokyo) 6 September 2021. Access Date: 6 January 2022. https://japan.kantei.go.jp/99_suga/actions/202109/_00012.html

[2411] New Digital Agency Pursues Inclusive Digitalization, The Government of Japan (Tokyo) 16 September 2021. Access Date: 6 January 2022. https://www.japan.go.jp/kizuna/2021/09/new_digital_agency.html

[2412] Signing of the Agreement between the Government of Japan and the Government of the Socialist Republic of Vietnam concerning the Transfer of Defense Equipment and Technology, Ministry of Foreign Affairs of Japan (Tokyo) 13 September 2021. Access Date: 27 January 2022. https://www.mofa.go.jp/press/release/press3e_000244.html

[2413] Japan, U.S., Australia to build 5G networks in South Pacific, Kyodo News (Tokyo) 13 December 2021. Access Date: 17 January 2022. https://english.kyodonews.net/news/2021/12/259bdb572d59-japan-us-australia-to-build-5g-networks-in-south-pacific.html

[2414] Digital Society Promotion Council, Prime Minister of Japan and His Cabinet (Tokyo) 24 December 2021. Access Date: 14 January 2022. https://japan.kantei.go.jp/101_kishida/actions/202112/_00024.html

Japan has fully complied with its commitment to preserve an open, interoperable, reliable and secure internet, one that is unfragmented, supports freedom, innovation and trust which empowers people. Japan's establishment of cyber security standards, government agencies focusing on digitalization and the funding of new undersea cable networks preserves an internet that is open, reliable, secure, and unfragmented.

Thus, Japan receives a score of +1.

Analyst: Arees Chooljian

United Kingdom: +1

The United Kingdom has fully complied with its commitment to preserve an open, interoperable, reliable, and secure internet that is unfragmented, supports freedom, innovation and trust which empowers people.

On 29 October 2021, Digital Secretary Nadine Dorries announced a plan to give more than 500,000 rural homes and businesses access to improved internet connectivity as part of Project Gigabit.[2415] Full fibre broadband cables will be installed in hard-to-reach rural areas to improve internet speed and reliability, which will allow more people to work from home and use the internet for leisure.

On 29 November 2021, the UK government signed agreements promoting digital trade facilitation at the Future Tech Forum.[2416] The agreement aims to promote an open and secure cyberspace and interoperable networks where companies can mix and match equipment from various vendors to boost security and drive innovation in the telecoms supply chain.

On 8 December 2021, the UK government announced plans to phase out 2G and 3G networks and replace them with 5G.[2417] The change aims to reduce the world's over-reliance on a few equipment makers and promote competition among telecoms. Secretary Dorries also announced a GBP50 million investment towards telecoms research and development projects.

On 15 December 2021, the UK government published National Cyber Strategy 2022.[2418] The new policy paper aims to reduce cyber risks to ensure citizens and businesses can confidently use the internet knowing their confidential data is protected. The strategy is built around five core pillars: deepen the relationship between government, academia and industry; reduce cyber risks for businesses and citizens; develop domestic industrial capabilities and secure future technological advancements; advance the UK's role as an industry global leader and enhance UK security in and through cyberspace.

On 4 January 2022, the National Security and Investment Act was announced to impose certain conditions for the government to intervene in the UK's national security.[2419] This act will also allow for investors to gain transparency in free trade and acquisitions.

[2415] Better broadband for 500,000 rural homes in UK gigabit revolution, Department for Digital, Culture, Media & Sport (London) 29 October 2021. Access Date: 30 January 2022. https://www.gov.uk/government/news/better-broadband-for-500000-rural-homes-in-uk-gigabit-revolution

[2416] UK signs series of international digital agreements at first Future Tech Forum, Department for Digital, Culture, Media & Sport (London) 29 November 2021. Access Date: 30 January 2022. https://www.gov.uk/government/news/uk-signs-series-of-international-digital-agreements-at-first-future-tech-forum

[2417] New Measures to boost UK telecom security, Department for Digital, Culture, Media & Sport (London) 8 December 2021. Access Date: 15 December 2021. https://www.gov.uk/government/news/new-measures-to-boost-uk-telecoms-security

[2418] National Cyber Strategy 2022, Cabinet Office (London) 15 December 2021. Access Date: 30 January 2022. https://www.gov.uk/government/publications/national-cyber-strategy-2022

[2419] New laws to strengthen national security come into effect, Department for Business, Energy & Industrial Strategy (London) 4 January 2022. Access Date: 10 January 2022. https://www.gov.uk/government/news/new-laws-to-strengthen-national-security-come-into-effect

The United Kingdom has fully complied with its commitment to preserve an open, interoperable, reliable and secure internet that is unfragmented, supports freedom, innovation and trust which empowers people. The UK has introduced policies and allocated funds in support of telecoms projects, national security and cyber-crime prevention. These policies promote safe and confident internet usage by businesses and the public.

Thus, the United Kingdom receives a score of +1.

Analyst: Selina Zeng

United States: +1

The United States has fully complied with its commitment to preserve an open, interoperable, reliable and secure internet, one that is unfragmented, supports freedom, innovation and trust which empowers people.

On 29 June 2021, the Federal Communications Commission (FCC) launched the Emergency Connectivity Fund.[2420] Schools can apply for financial support for purchasing laptops, tablets, routers and broadband connections to meet the needs for off-campus use by students and staff. Schools and libraries can also apply for the USD7.1 billion Emergency Connectivity Fund. The Fund will reduce the digital equity gap by supporting students who fall into the homework gap.

On 13 July 2021, the Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive to mitigate a Microsoft Windows print spooler vulnerability being exploited.[2421] The directive instructed federal civilian agencies to disable the service, apply the Microsoft updates and make configuration changes to all Microsoft Windows servers and workstations. If left unmitigated, the exploitation of this vulnerability could lead to the full system of affected agency networks being compromised.

On 23 July 2021, the FCC granted 5,676 C-Band Spectrum Licenses.[2422] The licenses pave the way for carriers to use this spectrum to provide advanced wireless services such as 5G.

On 26 July 2021, the FCC made over USD311 million available for broadband in 36 states through the Rural Digital Opportunity Fund.[2423] 48 broadband providers will provide broadband speeds of one gigabit per second (gbps) to 200,000 houses and businesses over the next decade.

On 28 July 2021, the FCC announced that over 4 million households were enrolled in the Emergency Broadband Benefit Fund.[2424] The fund is the largest broadband affordability program in the US with 1,100 broadband providers agreeing to partake in the program to temporarily subsidize eligible households' internet bills during the COVID-19 pandemic.

[2420] Federal Communications Commission Launches Country's Largest Effort To Close Homework Gap, Federal Communications Commission (Washington) 29 June 2021. Access Date: 20 November 2021. https://www.fcc.gov/document/fcc-launches-emergency-connectivity-fund

[2421] Cybersecurity and Infrastructure Security Agency issues emergency directive requiring federal agencies to mitigate windows print spooler service vulnerability, Cybersecurity and Infrastructure Security Agency (Washington) 13 July 2021. Access Date: 20 November 2021. https://www.cisa.gov/news/2021/07/13/cisa-issues-emergency-directive-requiring-federal-agencies-mitigate-windows-print

[2422] Federal Communications Commission Grants C-Band Spectrum Licenses, Federal Communications Commission (Washington) 23 July 2021. Access Date: 20 November 2021. https://www.fcc.gov/document/fcc-grants-c-band-spectrum-licenses

[2423] Federal Communications Commission Makes Available Over $311 Million For Broadband In 36 States, While Taking Steps To Clean Up The Rural Digital Opportunity Fund Program, Federal Communications Commission (Washington) 26 July 2021. Access Date: 20 November 2021. https://www.fcc.gov/document/fcc-announces-over-311-million-broadband-acts-clean-rdof

[2424] Federal Communications Commission Enrolls Over 4 Million Households In Emergency Broadband Benefit Program, Federal Communications Commission (Washington) 28 July 2021. Access Date: 20 November 2021. https://www.fcc.gov/document/fcc-enrolls-4m-households-emergency-broadband-benefit-program

On 2 August 2021, CISA announced the extension of the Information and Communications Technology Supply Chain Risk Management Task Force to 2023.[2425] The task force is a public-private partnership that identifies challenges and develops solutions and recommendations for risk management of the global information and communications technology supply chain.

On 5 August 2021, CISA announced a Joint Cyber Defense Collaboration (JCDC) to develop and execute cyber defense operations plans.[2426] JCDC's partners include Amazon Web Services, Microsoft and Verizon. CISA aims to facilitate coordinated action and implement defensive cyber operations to prevent cyber intrusions.

On 23 August 2021, the FCC granted six spectrum licenses to Tribal entities in Alaska.[2427] The licenses enable rural Alaska Native communities to use 5G and other advanced wireless services.

On 7 September 2021, CISA released the Cloud Security Technical Reference Architecture (TRA) and Zero Trust Maturity Model for public comment.[2428] The TRA guides agencies on zero trust strategies and implementation plans. CISA will work with stakeholders to assess feedback and develop new versions of guidance documents.

On 22 September 2021, CISA, the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) released a cybersecurity advisory.[2429] The advisory outlines technical steps on mitigating threats that public and private sector organizations can take to reduce risk to ransomware.

On 24 September 2021, the FCC announced that it will commit over USD1.2 billion in the first funding wave for the Emergency Connectivity Fund Program.[2430] The funds will go to over 3,040 schools, 260 libraries and 24 consortia. They will be used to provide students, school staff and librarians access to broadband connectivity and necessary devices for off-campus learning. The funds will support over 3 million devices and 774,115 broadband connections.

[2425] Cybersecurity and Infrastructure Agency announces renewal of the information and communications technology supply chain risk management task force, Cybersecurity and Infrastructure Security Agency (Washington) 2 August 2021. Access Date: 20 November 2021. https://www.cisa.gov/news/2021/08/02/cisa-announces-renewal-information-and-communications-technology-ict-supply-chain

[2426] Cybersecurity and Infrastructure Security Agency launches new joint cyber defense collaborative, Cybersecurity and Infrastructure Security Agency (Washington) 5 August 2021. Access Date: 20 November 2021. https://www.cisa.gov/news/2021/08/05/cisa-launches-new-joint-cyber-defense-collaborative

[2427] Federal Communications Commission Grants Additional 2.5 GHz Spectrum Licenses For Wireless Services In Alaska Native Communities, Federal Communications Commission (Washington) 23 August 2021. Access Date: 20 November 2021. https://www.fcc.gov/document/fcc-grants-licenses-wireless-services-alaska-native-communities

[2428] Cybersecurity and Infrastructure Agency releases the Cloud Security Technical Reference Architecture and Zero Trust Maturity Model for public comment, Cybersecurity and Infrastructure Security Agency (Washington) 7 September 2021. Access Date: 20 November 2021. https://www.cisa.gov/news/2021/09/07/cisa-releases-cloud-security-technical-reference-architecture-and-zero-trust

[2429] Cybersecurity and Infrastructure Agency, Federal Bureau of Investigation, and National Security Agency release conti ransomware to help organizations reduce risk of attack, Cybersecurity and Infrastructure Security Agency (Washington) 22 September 2021. Access Date: 20 November 2021. https://www.cisa.gov/news/2021/09/22/cisa-fbi-and-nsa-release-conti-ransomware-advisory-help-organizations-reduce-risk

[2430] Federal Communications Commission Commits Over $1.2 Billion In First Funding Wave Of Emergency Connectivity Fund Program To Connect Over 3.6 Million Students, Federal Communications Commission (Washington) 24 September 2021. Access Date: 20 November 2021. https://www.fcc.gov/document/fcc-commits-over-12b-first-emergency-connectivity-funding-wave

On 28 September 2021, the CISA released an Insider Risk Mitigation Self-Assessment Tool that helps public and private sector organizations assess their vulnerability to insider threats.[2431] The tool also helps organizations create prevention and mitigation programs to address insider threats.

On 12 October 2021, the FCC committed over USD1.1 billion in the second funding wave for the Emergency Connectivity Fund Program.[2432] The funds will support 2,471 schools, 205 libraries, and 26 consortia.

On 18 October 2021, the CISA, FBI and NSA released a cybersecurity advisory for BlackMatter ransomware cyber intrusions.[2433] The cyber intrusions were targeting entities such as US food and agriculture organizations. The advisory included technical details, assessment and mitigation actions to deal with the risk.

On 20 October 2021, the FCC announced that it will deploy USD554 million through the Rural Digital Opportunity Fund and provide broadband in 19 states.[2434] The FCC is also working to ensure that the funding goes to qualified providers in areas that need broadband.

On 20 October 2021, the CISA awarded USD 2 million to NPower and CyberWarrior, which are organizations working on the development of cyber workforce training programs.[2435] This is a part of CISA's mission to build the workforce of the future. The organizations work on underprivileged communities, veterans, military spouses, unemployed people and underemployed people.

On 25 October 2021, the FCC committed an additional USD269 million to the Emergency Connectivity Fund Program.[2436] The program received nearly USD1.3 billion in funding requests in the second application filing window. The funds will be used for connected devices and broadband connections.

On 26 October 2021, the FCC announced the third set of projects selected for the Connected Care Pilot Program.[2437] The program will support connected care technologies and services all over the US. It particularly focuses on low-income and veteran patients.

[2431] Cybersecurity and Infrastructure Agency released new tool to help organizations guard against insider threats, Cybersecurity and Infrastructure Security Agency (Washington) 28 September 2021. Access Date: 20 November 2021. https://www.cisa.gov/news/2021/09/28/cisa-releases-new-tool-help-organizations-guard-against-insider-threats

[2432] Federal Communications Commission Commits Over $1.1 Billion In Second Funding Wave Of Emergency Connectivity Fund Program, Funding Over 2.4 Million Devices And 1.9 Million Broadband Connections, Federal Communications Commission (Washington) 12 October 2021. Access Date: 20 November 2021. https://www.fcc.gov/document/fcc-commits-another-11-billion-emergency-connectivity-fund

[2433] Cybersecurity and Infrastructure Agency, Federal Bureau of Investigation and National Security Agency release BlackMatter ransomware advisory to help organizations reduce risk of attack, Cybersecurity and Infrastructure Security Agency (Washington) 18 October 2021. Access Date: 20 November 2021. https://www.cisa.gov/news/2021/10/18/cisa-fbi-and-nsa-release-blackmatter-ransomware-advisory-help-organizations-reduce

[2434] Federal Communications Commission Announces $554 Million For Broadband In 19 States Through Rural Digital Opportunity Fund Program, Federal Communications Commission (Washington) 20 October 2021. Access Date: 20 November 2021. https://www.fcc.gov/document/fcc-announces-554-million-broadband-19-states

[2435] Cybersecurity and Infrastructure Agency awards $2 million to bring cybersecurity training to rural communities and diverse populations, Cybersecurity and Infrastructure Security Agency (Washington) 20 October 2021. Access Date: 20 November 2021. https://www.cisa.gov/news/2021/10/20/cisa-awards-2-million-bring-cybersecurity-training-rural-communities-and-diverse

[2436] Federal Communications Commission Announces Nearly $1.3 Billion In Funding Requests Received In Emergency Connectivity Fund Program Second Application Filing Window, Federal Communications Commission (Washington) 25 October 2021. Access Date: 20 November 2021. https://www.fcc.gov/document/fcc-receives-13b-new-emergency-connectivity-fund-applications

[2437] Federal Communications Commission Announces Third Set of Projects Selected for the Connected Care Pilot Program, Federal Communications Commission (Washington) 27 October 2021. Access Date: 20 November 2021. https://www.fcc.gov/document/fcc-announces-36-newly-approved-connected-care-pilot-program-projects-0

On 28 October 2021, the CISA and NSA released cybersecurity guidance to build and configure secure cloud infrastructures to support 5G.[2438] The release is part of the Enduring Security Framework's four part series to provide cybersecurity guidance pertaining to high priority cyber threats to critical infrastructure.

On 29 October 2021, the FCC approved 20 spectrum licenses for the Alaskan Native communities.[2439] This allows underserved rural Tribal communities to use advanced wireless technologies.

On 3 November 2021, the FCC authorized the Boeing Company to construct, deploy and operate a satellite constellation.[2440] The satellite will provide broadband and communication services for commercial, governmental and residential use in the US and globally.

On 8 November 2021, the FCC committed additional funding of over USD421 million through the Emergency Connectivity Fund Program.[2441] The new funding will allow a total of 10 million students to be connected to reliable internet.

On 10 November 2021, the FCC announced over USD700 million in funding for broadband through the Rural Digital Opportunity Fund.[2442] The funding will provide broadband for over 26 states and ensure that qualified providers serve areas that require broadband.

On 16 November 2021, the CISA released the Federal Government Cybersecurity Incident and Vulnerability Response Playbooks which provide federal civilian agencies with guidelines on responding to vulnerabilities and incidents.[2443] This information will help federal agencies identify and recover from incidents and vulnerabilities.

On 18 November 2021, the CISA and NSA published guidelines to mitigate cyber threats within 5G cloud infrastructure.[2444] The guidance includes pod security such as avoiding resource contention and implementing real time threat detection.

On 19 November 2021, the FCC proposed an enhanced competition incentive program to encourage licensees to lease, partition or disaggregate spectrum to small carriers and tribal nations.[2445] The proposal also outlined incentives for licensees such as license term extensions and construction extensions.

[2438] National Security Agency and Cybersecurity and Infrastructure Agency provide cybersecurity for 5G cloud infrastructures, Cybersecurity and Infrastructure Security Agency (Washington) 28 October 2021. Access Date: 20 November 2021. https://www.cisa.gov/news/2021/10/28/nsa-and-cisa-provide-cybersecurity-guidance-5g-cloud-infrastructures

[2439] Federal Communications Commission Approves Additional 2.5 GHz Spectrum Licenses To Serve Alaska Native Communities, Federal Communications Commission (Washington) 29 October 2021. Access Date: 20 November 2021. https://www.fcc.gov/document/fcc-approves-spectrum-licenses-serve-alaska-native-communities

[2440] Federal Communications Commission Authorizes Boeing Broadband Satellite Constellation, Federal Communications Commission (Washington) 3 November 2021. Access Date: 20 November 2021. https://www.fcc.gov/document/fcc-authorizes-boeing-broadband-satellite-constellation

[2441] Federal Communications Commission Commits Over $421 Million In Additional Funding Through Emergency Connectivity Fund Program, Federal Communications Commission (Washington) 8 November 2021. Access Date: 20 November 2021. https://www.fcc.gov/document/fcc-commits-421-million-additional-emergency-connectivity-funding

[2442] Federal Communications Commission Announces Over $700 Million For Broadband In 26 States Through Rural Digital Opportunity Fund, Federal Communications Commission (Washington) 10 November 2021. Access Date: 20 November 2021. https://www.fcc.gov/document/fcc-announces-over-700-million-broadband-26-states

[2443] Cybersecurity and Infrastructure Agency releases incident and vulnerability response playbooks to strengthen cybersecurity for federal civilian agents, Cybersecurity and Infrastructure Security Agency (Washington) 16 November 2021. Access Date: 20 November 2021. https://www.cisa.gov/news/2021/11/16/cisa-releases-incident-and-vulnerability-response-playbooks-strengthen

[2444] Enduring security framework releases part II of security guidance for 5G cloud infrastructures, Cybersecurity and Infrastructure Security Agency (Washington) 18 November 2021. Access Date: 20 December 2021. https://www.cisa.gov/news/2021/11/18/enduring-security-framework-releases-part-ii-security-guidance-5g-cloud

On 22 November 2021, the FCC announced additional program integrity measures for the Emergency Benefit Program enrollments.[2446] The measures, based on the community eligibility provision, aim to strengthen program integrity.

On 23 November 2021, the FCC committed over USD169 million to the Emergency Connectivity Fund.[2447] The funding provides support to over 500,000 students in 47 states. The funding will support 492 schools, 70 libraries, and 10 consortia. They will receive over 135,000 broadband connections.

On 1 December 2021, Director of CISA Jen Easterly announced the appointment of 23 members to the Cybersecurity Advisory Committee.[2448] The Committee will provide recommendations on policies, training and programs to improve cyber defense and grow the cyber workforce.

On 16 December 2021, the FCC announced over USD1 billion for the Rural Digital Opportunity Fund.[2449] The funding will provide support for broadband in 32 states over 10 years. 69 broadband providers will provide broadband services to 518,088 locations in the 32 states.

On 17 December 2021, the Bureau of Democracy, Human Rights, and Labor (DRL) announced a Request for Statement of Interest from organizations interested in potential funding from DRL.[2450] DRL invites organizations to submit statement of interest applications and outline program concepts that work on protecting the "open, interoperable, secure and reliable" internet by promoting, among other initiatives, the free flow of information and digital safety.

On 20 December 2021, FCC committed around USD603 million in additional Emergency Connectivity Funding.[2451] The program will connect over 1.4 million students in all 50 states, Puerto Rico and the District of Columbia and may be used to support off-campus learning.

On 22 December 2021, the CISA, FBI, NSA, Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), Computer Emergency Response Team New Zealand (CERT NZ), New Zealand National Cyber Security Centre (NZ NCSC), and the United Kingdom's National Cyber Security Centre issued

[2445] Partitioning, Disaggregation, and Leasing of Spectrum, WT Docket No. 19-38, Further Notice of Proposed Rulemaking, Federal Communications Commission (Washington) 19 November 2021. Access Date: 20 December 2021. https://www.fcc.gov/document/fcc-proposes-enhanced-competition-incentive-program-0

[2446] Wireline Competition Bureau Announces Additional Program Integrity Measures for Emergency Benefit Program Enrollments Based on the Community Eligibility Provision, Federal Communications Commission (Washington) 22 November 2021. Access Date: 20 December 2021. https://www.fcc.gov/document/wcb-implements-ebb-program-integrity-measures-cep-enrollments

[2447] Federal Communications Commission Commits Over $169 Million in Additional Emergency Connectivity Fund Support, Federal Communications Commission (Washington) 23 November 2021. Access Date: 20 December 2021. https://www.fcc.gov/document/fcc-commits-over-169m-emergency-connectivity-funding

[2448] CISA names 23 members to new cybersecurity advisory committee, Cybersecurity and Infrastructure Security Agency (Washington) 1 December 2021. Access Date: 20 December 2021. https://www.cisa.gov/news/2021/12/01/cisa-names-23-members-new-cybersecurity-advisory-committee

[2449] Federal Communications Commission Announces Over $1 Billion in Rural Digital Opportunity Fund Support for Broadband in 32 States as Commission Continues To Clean Up Program, Federal Communications Commission (Washington) 16 December 2021. Access Date: 20 December 2021. https://www.fcc.gov/document/fcc-announces-over-1-billion-rural-broadband-support-32-states

[2450] Requests for Statements of Interest: DRL FY22 Internet Freedom Annual Program Statement, U.S Department of State (Washington) 17 December 2021. Access Date: 26 December 2021. https://www.state.gov/request-for-statements-of-interest-drl-fy22-internet-freedom-annual-program-statement/

[2451] Federal Communications Commission commits nearly $603M in additional emergency connectivity funding, Federal Communications Commission (Washington) 20 December 2021. Access Date: 26 December 2021. https://www.fcc.gov/document/fcc-commits-nearly-603m-additional-emergency-connectivity-funding an advisory on vulnerabilities in the Apache Log4j software.[2452] The advisory includes technical details and resources for potentially impacted organizations to address vulnerabilities. The advisory was issued in response to cyber threat actors exploiting vulnerabilities found in Java-based logging package Log4j.

On 10 January 2022, the CISA published its Public Safety Communications Security white paper which explains the importance and basic elements of Communications Security.[2453] The paper explains how to develop an effective strategy to prevent unauthorized persons from accessing sensitive and confidential information.

The United States has fully complied with its commitment to preserve an open, interoperable, reliable and secure internet, one that is unfragmented, supports freedom, innovation and trust which empowers people. The US took steps to provide unrestricted access to the internet by reaching tribal communities, students in need and collaborated with Boeing to provide internet access globally. The US also took steps to strengthen cyber defense and set up innovation zones for research purposes. The US granted spectrum licenses, increased broadband access to rural areas, aided Alaskan communities and empowered small carriers and tribal nations by incentivizing licensees to lease spectrum.

Thus, the United States receives a score of +1.

Analyst: Sarah Nasir

European Union: +1

The European Union has fully complied with its commitment to preserve an open, interoperable, reliable and secure internet that is unfragmented, supports freedom, innovation and trust which empowers people.

On 19 July 2021, the EU assessed and exposed malicious cyber activities that affected the EU's economy, security, democracy and society after hackers compromised and exploited the Microsoft Exchange server.[2454] Other cyber activities that targeted government institutions and political organizations were also identified. The activities were linked to hacker groups and had been conducted from the territory of China. The EU urged Chinese authorities to implement measures to investigate the situation.

On 28 July 2021, the European Data Protection Board (EDPB) requested the Irish Supervisory Authority (IE SA) to amend its draft decision regarding transparency infringements.[2455] The EDPB adopted a dispute resolution decision which addresses the dispute following a draft decision issued by the IE SA regarding WhatsApp Ireland Ltd. The EDPB identified breaches of articles by the IE AS and believed the IE SA should amend its draft decision pertaining to the infringements of transparency, calculation of fine and period for the order to comply.

[2452] Cybersecurity and Infrastructure Agency, Federal Bureau of Investigation, National Security Agency and international partners issue advisory to mitigate apache log4k vulnerabilities, Cybersecurity and Infrastructure Security Agency (Washington) 22 December 2021. Access Date: 26 December 2021. https://www.cisa.gov/news/2021/12/22/cisa-fbi-nsa-and-international-partners-issue-advisory-mitigate-apache-log4j

[2453] The Cybersecurity and Infrastructure Agency has published its public safety communications security white paper, Cybersecurity and Infrastructure Agency (Washington) 10 January 2022. Access Date: 16 January 2022. https://www.cisa.gov/blog/2022/01/10/cybersecurity-and-infrastructure-security-agency-cisa-has-published-its-public-0

[2454] China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory, European Council (Brussels) 19 July 2021. Access Date: 20 November 2021. https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/

[2455] European Data Protection Board requests that Irish SA amends WhatsApp decision with clarifications on transparency and on the calculation of the amount of fine due to multiple infringements, European Data Protection Board (Brussels) 2 September 2021. Access Date: 20 November 2021. https://edpb.europa.eu/news/news/2021/edpb-requests-irish-sa-amends-whatsapp-decision-clarifications-transparency-and_en

On 27 September 2021, the EDPB set up a taskforce in response to complaints concerning cookie banners filed with several European Economic Area (EEA) SAs.[2456] The task force will streamline communication between SAs and exchange views on legal analysis and potential infringements.

On 18 October 2021, the EDPB launched the proposal for its first coordinated action on the use of Cloud based services by the public sector.[2457] SAs work on certain topics at the national level and the results of the actions will be analyzed for deeper insight on the topic, which will allow for a more targeted follow-up at the national and EU level.

On 13 October 2021, the EDPB adopted the final version of Guidelines on the restrictions of data subject rights under Article 23 GDPR following a public consultation.[2458] The guidelines provide a thorough analysis of criteria to apply restrictions and how data subjects can exercise their rights.[2459]

On 19 October 2021, the European Commission proposed the Cyber Resilience Act.[2460] The Act will establish common cybersecurity standards, provide EU-wide broadband connectivity and secure independent communications to member states.

On 20 October 2021, the European Parliament called for the extension of the EU's roam like at home policy, which ensures that Europeans can continue to use mobile data anywhere in the EU at no extra cost.[2461] The new legislation will extend the policy for another ten years and ensure that networks with equivalent speed and quality to those they would use at home are available to travelers.

On 28 October 2021, the Industry Committee adopted a new draft legislation that would set stricter cybersecurity obligations.[2462] The legislation would require EU members to take stricter supervisory and enforcement measures in digital infrastructure, health and banking sectors. Important sectors such as postal services would also be protected by the new law. The legislation calls for stricter risk management, reporting obligations and information sharing to protect against cybercrime and make the EU "a safe place to work and do business."

On 20 November 2021, the European External Action Service (EEAS) and the Ombudsperson for Children Office in Mauritius published a leaflet on key actions to fight online child sexual abuse.[2463] The EEAS also

[2456] European Data Protection Board establishes cookie banner task force, European Data Protection Board (Brussels) 27 September 2021. Access Date: 20 November 2021. https://edpb.europa.eu/news/news/2021/edpb-establishes-cookie-banner-taskforce_en

[2457] European Data Protection Board launches first coordinated action, European Data Protection Board (Brussels) 18 October 2021. Access Date: 20 November 2021. https://edpb.europa.eu/news/news/2021/edpb-launches-first-coordinated-action_en

[2458] Guidelines 10/2020 on restrictions under Article 23 GDPR, European Data Protection Board (Brussels) n.d. Access Date: 30 January 2022. https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf

[2459] European Data Protection Board adopts Guidelines on restrictions of data subject rights under Article 23 GDPR following public consultation, European Data Protection Board (Brussels) 19 October 2021. Access Date: 20 November 2021. https://edpb.europa.eu/news/news/2021/edpb-adopts-guidelines-restrictions-data-subject-rights-under-article-23-gdpr_en

[2460] 2022 Commission Work Programme: Making Europe stronger together, European Commission (Brussels) 19 October 2021. Access Date: 20 November 2021. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_5246

[2461] Roam like at home: Parliament backs roaming extension, European Parliament (Strasbourg) 20 October 2021. Access date: 20 November 2021. https://www.europarl.europa.eu/news/en/headlines/society/20211015STO15005/roam-like-at-home-parliament-backs-roaming-extension

[2462] Cybersecurity: Members of European Parliament strengthen EU-wide requirements against threats, European Parliament (Strasbourg) 28 October 2021. Access date: 20 November 2021. https://www.europarl.europa.eu/news/en/press-room/20211022IPR15610/cybersecurity-meps-strengthen-eu-wide-requirements-against-threats

[2463] RIGHTS OF THE CHILD: Protecting our children online, European Union Action Service (Brussels) 20 November 2021. Access Date: 20 December 2021. https://eeas.europa.eu/headquarters/headquarters-homepage/107585/rights-child-protecting-our-children-online_en produced a video clip that will be broadcast on national television in Mauritius to spread awareness to children, teachers and parents on the dangers of the internet.

On 3 December 2021, the European Council agreed on its position to replace the Network and Information Systems (NIS) directive with the NIS2 directive, which will set the baselines for reporting obligations and cyber security risk management measures.[2464] Once adopted, the NIS2 will improve incident response capacities of the public and private sectors.

On 14 December 2021, the European Parliament Internal Market and Consumer Protection Committee adopted the Digital Services Act (DSA).[2465] The DSA creates safer online platforms by protecting fundamental rights online.[2466] The DSA includes new rules to tackle illegal content through a 'notice and action' mechanism and safeguards.[2467] It aims to prevent the spread of harmful content through algorithms by making sure platforms are transparent about the way algorithms work. They will be required to carry out risk assessments and take risk mitigation measures. Digital service recipients on large online platforms will also have the right to seek compensation for damages resulting from platforms not respecting their obligations.

On 14 December, the European Parliament passed the Digital Markets Act (DMA).[2468] The proposal was adopted by the Internal Market and Consumer Protection Committee in November.[2469] The DMA levels the playing field for all digital companies irrespective of size.[2470] The major companies of gatekeepers will be identified and will have to refrain from imposing unfair conditions on businesses and consumers.[2471] The gatekeepers may also be restricted from making acquisitions.

On 16 December 2021, the European Commission adopted the Work Programme for the Connecting Europe Facility (CEF Digital).[2472] The European Commission will provide more than EUR1 billion in funding for the actions of CEF Digital. These actions include deploying 5G across the EU, fostering public and private investments, upgrading existing networks and implementing digital connectivity infrastructures.

[2464] Strengthening EU-wide cybersecurity and resilience – Council agrees its position, European Council (Brussels) 3 December 2021. Access Date: 20 December 2021. https://www.consilium.europa.eu/en/press/press-releases/2021/12/03/strengthening-eu-wide-cybersecurity-and-resilience-council-agrees-its-position/

[2465] Digital Services Act: a safer online space for users, stricter rules for platforms, European Parliament (Strasbourg) 14 December 2021. Access Date: 25 December 2021. https://www.europarl.europa.eu/news/en/press-room/20211210IPR19209/digital-services-act-safer-online-space-for-users-stricter-rules-for-platforms

[2466] EU Digital Markets Act and Digital Services Act explained, European Parliament (Strasbourg) 14 December 2021. Access Date: 25 December 2021. https://www.europarl.europa.eu/news/en/headlines/society/20211209STO19124/eu-digital-markets-act-and-digital-services-act-explained

[2467] Digital Services Act: a safer online space for users, stricter rules for platforms, European Parliament (Strasbourg) 14 December 2021. Access Date: 25 December 2021. https://www.europarl.europa.eu/news/en/press-room/20211210IPR19209/digital-services-act-safer-online-space-for-users-stricter-rules-for-platforms

[2468] EU Digital Markets Act and Digital Services Act explained, European Parliament (Strasbourg) 14 December 2021. Access Date: 25 December 2021. https://www.europarl.europa.eu/news/en/headlines/society/20211209STO19124/eu-digital-markets-act-and-digital-services-act-explained

[2469] Digital Markets Act: ending unfair practices of big online platforms, European Parliament (Strasbourg) 23 November 2021. Access Date: 20 December 2021. https://www.europarl.europa.eu/news/en/press-room/20211118IPR17636/digital-markets-act-ending-unfair-practices-of-big-online-platforms

[2470] EU Digital Markets Act and Digital Services Act explained, European Parliament (Strasbourg) 14 December 2021. Access Date: 25 December 2021. https://www.europarl.europa.eu/news/en/headlines/society/20211209STO19124/eu-digital-markets-act-and-digital-services-act-explained

[2471] Digital Markets Act: ending unfair practices of big online platforms, European Parliament (Strasbourg) 23 November 2021. Access Date: 20 December 2021. https://www.europarl.europa.eu/news/en/press-room/20211118IPR17636/digital-markets-act-ending-unfair-practices-of-big-online-platforms

[2472] Commission to invest for than 1 billion under the connecting Europe facility for innovative and secure connectivity, European Commission (Brussels) 16 December 2021. Access Date: 20 December 2021. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_6830

The European Union has fully complied with its commitment to preserve an open, interoperable, reliable and secure internet that is unfragmented, supports freedom, innovation and trust which empowers people. The EU took steps to increase access to the internet through broadband connectivity advancement and enhanced cyber security measures and streamlined communication between businesses. The EU also empowered internet users and businesses by mandating more transparency from online platforms.

Thus, the European Union receives a score of +1.

Analyst: Sarah Nasir